

Functional boxes, communication complexity and information causality

Guoming Wang^{1,*}

¹*Computer Science Division, University of California Berkeley, Berkeley, California 94720, USA*
(Dated: September 30, 2011)

We propose a class of nonlocal boxes named functional boxes which include a generalization of the Popescu-Rohrlich (PR) box as a special case. We show that every functional box corresponding to an additively inseparable function can make communication complexity trivial and thus seems unlikely to exist in nature. Then we relate general nonlocal boxes to these functional boxes, and derive several limits on them from the principle of information causality.

PACS numbers: 03.65.Ud

I. INTRODUCTION

Quantum mechanics allows distant parties to establish certain correlations that are impossible in the classical world. These correlations are nonlocal, in the sense that they violate Bell inequality [1, 2]. However, as first shown by Tsirelson [3], their violation is still bounded. In a seminal paper, Popescu and Rohrlich [4] proposed a hypothetical nonlocal correlation that attains the maximal value for the Clauser-Horne-Shimony-Holt (CHSH) inequality [2] but still cannot be used to signal from one party to another. Understanding why such stronger-than-quantum correlations have not been observed in nature has since then become an active topic of research [5–31]. Recently, several information-theoretical principles were proposed as candidates that separate physically realizable correlations from nonphysical ones. In this paper, we will be concerned with two of them — nontrivial communication complexity [5] and information causality [18]. Both of them show that allowing certain postquantum correlations would lead to implausible simplification of communication tasks.

In one line, van Dam [5] showed that, equipped with many copies of Popescu-Rohrlich (PR) boxes [4], every communication complexity problem can be solved deterministically by a single bit of communication. Then, Brassard *et al.* [10] extended this result by proving that if PR boxes can be implemented with probability greater than $(3 + \sqrt{6})/6 \approx 90.8\%$, then the probabilistic communication complexity also collapses. These results were further generalized by Refs. [7, 16, 19].

In another line, Pawłowski *et al.* [18] considered a scenario in which Alice had a database of N independent and random bits, and a distant party, Bob, was asked to guess the k -th bit in Alice's database for random $k \in \{0, 1, \dots, N-1\}$. They suggested a principle stating that Bob can gain at most m bits of information about Alice's database by using his local resources and receiving m bits from Alice. This principle was named information causality. When $m = 0$, it reduces to no-signalling. It

was demonstrated that using many copies of PR boxes Bob can correctly guess any bit of Alice with certainty by receiving only 1 bit from her. Moreover, any correlation exceeding Tsirelson's bound for the CHSH inequality violates information causality. The implications of information causality on nonlocality were further explored in Refs. [21, 23, 27–31].

A common feature of these two proposals is that the PR box perfectly cracks the information processing task under consideration. It also exhibits an extremely strong power for other tasks [6, 14]. The reason for the success of this box can be summarized as follows. Essentially, the aforementioned tasks can be viewed as that Alice and Bob want to compute some function $f(x, y)$ in some distributed way, where x and y are initially held by Alice and Bob respectively. Note that any boolean (or arithmetic) function can be computed by a circuit consisting of XOR (or addition) and AND (or multiplication) gates. These two types of gates generally do not commute. However, using a PR box, AND operations are “transformed” into XOR operations, in the way that the AND of two inputs is encoded as the XOR of two outputs. So Alice and Bob effectively convert the original circuit into a “circuit” consisting of only XOR operations, which are commutative. Then Alice and Bob can reorder their operations, compact them, and minimize the interaction between them. This argument was made explicit in the discussion of communication complexity [5]. But it can also explain the success of PR box for the information causality task, since that task can be viewed as the communication complexity problem for a special function — the index function $f(\vec{x}, y) \equiv x_y$, with the extra condition that the communication is only from Alice to Bob.

In light of the above observation, we introduce a class of nonlocal boxes called *functional boxes*. This class of boxes include a generalization of PR box as a special case. A functional box's inputs and outputs have p possible values which are identified with the elements of \mathbb{Z}_p , where p can be any prime number. This box encodes the value of a function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ over its inputs as the difference of its outputs. In particular, the PR box is just the functional box corresponding to $f(x, y) = xy$ and $p = 2$. We find that, as long as f is not *additively separable* (see section 2 for definition), the corresponding functional box is asymptotically equivalent to a general-

*Electronic address: gmwang@eecs.berkeley.edu

ized PR box. (More specifically, an additively inseparable function contains a component that is about the multiplication of its two variables, and we show that this component can be isolated out by using a difference method, and hence the corresponding functional box can be transformed into a generalized PR box.) We also prove that a generalized PR box can enable perfect distributed computation and make communication complexity trivial. As a result, any functional box equivalent to it has the same power and is unlikely to exist in nature. Then the next question is how well these functional boxes might be approximated. We derive several bounds on the proximity between a plausible p -nary-input, p -nary-output box and these functional boxes, from the principle of information causality. In order to do this, we extend the basic and nested protocols in Ref.[18] to the p -nary digit case. Besides, we also present a generalization of the *depolarization* process that transforms any binary-input binary-output box into an *isotropic* one[11, 32], which might be of independent interest.

II. FUNCTIONAL BOXES AND COMMUNICATION COMPLEXITY

Let us first review several basic definitions about non-local boxes.

Definition 1. A bipartite correlation box (or simply a box) is a hypothetical device shared by two spatial separated parties Alice and Bob that receives an input $x \in \mathcal{X}$ from Alice and an input $y \in \mathcal{Y}$ from Bob, and outputs $a \in \mathcal{A}$ to Alice and $b \in \mathcal{B}$ to Bob, according to a joint probability distribution $P(a, b|x, y)$. Without causing ambiguity, we also call this box P .

If P satisfies

$$\begin{aligned} \sum_b P(a, b|x, y) &= \sum_b P(a, b|x, y') \equiv P(a|x), \quad \forall a, x, y, y'; \\ \sum_a P(a, b|x, y) &= \sum_a P(a, b|x', y) \equiv P(b|y), \quad \forall b, x, x', y, \end{aligned} \quad (1)$$

then it is no-signalling. Namely, Alice cannot signal to Bob via her choice of input to this box and vice versa.

If Alice and Bob can simulate P using shared randomness (without communication between them), then P is local. Otherwise, it is nonlocal.

For example, the standard PR box is given by

$$PR(a, b|x, y) = \begin{cases} \frac{1}{2}, & \text{if } a \oplus b = x \wedge y \\ 0, & \text{otherwise} \end{cases}, \quad (2)$$

where $a, b, x, y \in \{0, 1\}$. Note that $PR(a|x, y) = PR(b|x, y) = \frac{1}{2}$, $\forall a, b, x, y$. So this box is no-signalling.

In this paper, we focus on no-signalling boxes for which $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{A}| = |\mathcal{B}| = p$, where p can be any prime number. Without loss of generality, we assume $\mathcal{X} = \mathcal{Y} =$

$\mathcal{A} = \mathcal{B} = \{0, 1, \dots, p-1\} \equiv \mathbb{Z}_p$, and all the following computation related to x, y, a, b is modulo p .

Definition 2. A function $F : \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p$ is distributedly computed by Alice and Bob if, when Alice is given any $\vec{x} = (x_0, x_1, \dots, x_{n-1}) \in \mathbb{Z}_p^n$ and Bob is given any $\vec{y} = (y_0, y_1, \dots, y_{m-1}) \in \mathbb{Z}_p^m$, Alice can produce $a \in \mathbb{Z}_p$ and Bob can produce $b \in \mathbb{Z}_p$ such that $a - b = F(\vec{x}, \vec{y})$.

If F can be distributedly computed with certainty (or with constant probability), then the deterministic (or probabilistic) communication complexity of F becomes trivial, since Alice can simply send a to Bob and then Bob can calculate $a - b = F(\vec{x}, \vec{y})$.

Let us first consider the following box, which is a straightforward generalization of standard PR box to the p -nary input/output case:

Definition 3.

$$PR_p(a, b|x, y) = \begin{cases} \frac{1}{p}, & \text{if } a - b = xy \\ 0, & \text{otherwise} \end{cases}, \quad (3)$$

where $a, b, x, y \in \mathbb{Z}_p$.

In particular, the standard PR box is just PR_2 . Note that $PR_p(a|x, y) = PR_p(b|x, y) = \frac{1}{p}$, $\forall a, b, x, y$. So PR_p is no-signalling.

Given arbitrarily many copies of PR_p , Alice and Bob will be able to distributedly compute any function $F : \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p$ perfectly. To prove this, first note that $F(\vec{x}, \vec{y})$ can always be written as a multivariate polynomial whose degree in each x_i or y_j is no larger than $p-1$:

$$F(\vec{x}, \vec{y}) = \sum_{\alpha_0, \dots, \alpha_{n-1}=0}^{p-1} \sum_{\beta_0, \dots, \beta_{m-1}=0}^{p-1} \mu_{\vec{\alpha}, \vec{\beta}} \prod_{i=0}^{n-1} x_i^{\alpha_i} \prod_{j=0}^{m-1} y_j^{\beta_j} \quad (4)$$

for some $\mu_{\vec{\alpha}, \vec{\beta}} \in \mathbb{Z}_p$, where $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ and $\vec{\beta} = (\beta_0, \beta_1, \dots, \beta_{m-1})$. So Alice and Bob can execute the following protocol: for each $(\vec{\alpha}, \vec{\beta})$, they use a PR_p as follows: Alice inputs $\prod_{i=0}^{n-1} x_i^{\alpha_i}$ and Bob inputs $\prod_{j=0}^{m-1} y_j^{\beta_j}$, and suppose they get outputs $a_{\vec{\alpha}, \vec{\beta}}$ and $b_{\vec{\alpha}, \vec{\beta}}$ respectively. In the end, Alice sets $a = \sum_{\vec{\alpha}} \sum_{\vec{\beta}} \mu_{\vec{\alpha}, \vec{\beta}} a_{\vec{\alpha}, \vec{\beta}}$ as her final output, and Bob sets $b = \sum_{\vec{\alpha}} \sum_{\vec{\beta}} \mu_{\vec{\alpha}, \vec{\beta}} b_{\vec{\alpha}, \vec{\beta}}$ as his final output. It is easy to verify $a - b = F(x, y)$.

Now let us consider a wider class of boxes:

Definition 4. For any function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, the functional box corresponding to f is defined as

$$P^f(a, b|x, y) = \begin{cases} \frac{1}{p}, & \text{if } a - b = f(x, y) \\ 0, & \text{otherwise} \end{cases}, \quad (5)$$

where $a, b, x, y \in \mathbb{Z}_p$.

Namely, P^f can be directly used to distributedly compute f . In particular, PR_p can be viewed as the functional box corresponding to $f(x, y) = xy$. Note that $P^f(a|x, y) = P^f(b|x, y) = \frac{1}{p}$, $\forall a, b, x, y$. So P^f is also no-signalling.

Definition 5. A bivariate function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is additively separable if there exist univariate functions $g, h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ such that $f(x, y) = g(x) + h(y)$, $\forall x, y \in \mathbb{Z}_p$. Otherwise, f is additively inseparable.

Definition 6. Suppose $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ can be written as $f(x, y) = \sum_{i,j=0}^{p-1} \lambda_{i,j} x^i y^j$ for some $\lambda_{i,j} \in \mathbb{Z}_p$. Define

$$\Delta(f) = \max_{1 \leq i,j \leq p-1} \{\mathbb{I}_{\lambda_{i,j} \neq 0}(i+j)\}, \quad (6)$$

where \mathbb{I} is the indicator function (i.e. $\mathbb{I}_E = 1$ if E is true, and 0 otherwise). Namely, $\Delta(f)$ is the maximum of the degrees of the terms in f that can be divided by xy .

Obviously, a function f is additively inseparable if and only if $\Delta(f) \geq 2$. Only an additively inseparable f contains a term that is related to the product of x and y . So one may naturally wonder if P^f can be used to simulate PR_p . If so, then P^f can also benefit distributed computation. We find that it is indeed the case, provided we are given sufficiently many copies of P^f .

Definition 7. We use the notation $P_1 \rightarrow P_2$ to denote the fact that we can use N copies of P_1 to simulate a P_2 exactly, for some $N \geq 1$. We also use $P_1 \leftrightarrow P_2$ to denote that $P_1 \rightarrow P_2$ and $P_2 \rightarrow P_1$, i.e. P_1 and P_2 are asymptotically interconvertible.

Lemma 8. If $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is additively separable, then P^f is local. Otherwise, $P^f \leftrightarrow PR_p$.

Proof: (1) Suppose $f(x, y) = g(x) + h(y)$ for some $g, h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, then we can build a local model for P^f as follows: Alice and Bob first generate a uniformly random variable $z \in \mathbb{Z}_p$, then Alice outputs $a = g(x) + z$ and Bob outputs $b = -h(y) + z$.

(2) Suppose f is additively inseparable. We first show $PR_p \rightarrow P^f$. Recall that we have already shown how to use many copies of PR_p to perform distributed computation of any functions, including f . So Alice and Bob can first use that protocol to obtain a and b such that $a - b = f(x, y)$. Then they generate a uniformly random $z \in \mathbb{Z}_p$ and modify their outputs by $a \rightarrow a + z$ and $b \rightarrow b + z$.

It remains to show $P^f \rightarrow PR_p$. Proof by induction on $\Delta(f)$:

- Base case: $\Delta(f) = 2$. In this case, we have

$$f(x, y) = \lambda xy + g(x) + h(y) \quad (7)$$

for some $\lambda \neq 0$ and $g, h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. We can use a P^f to simulate a PR_p as follows: Alice inputs x

and Bob inputs y to P^f , and suppose they obtain outputs a and b respectively. Then Alice sets

$$a' = \lambda^{-1}(a - g(x)) \quad (8)$$

as her final output, while Bob sets

$$b' = \lambda^{-1}(b + h(y)) \quad (9)$$

as his final output. Then we have

$$\begin{aligned} a' - b' &= \lambda^{-1}(a - b - g(x) - h(y)) \\ &= \lambda^{-1}(f(x, y) - g(x) - h(y)) \\ &= xy. \end{aligned} \quad (10)$$

Furthermore, since a (or b) is uniformly random, a' (or b') is also uniformly random conditioned on any (x, y) .

- Inductive step: Suppose $P^f \rightarrow PR_p$ for any f with $\Delta(f) = k$ for some $k \geq 2$. Consider any f with $\Delta(f) = k+1 \geq 3$. Such $f(x, y)$ (viewed as a bivariate polynomial) contains a term that is a multiple of x^2y or xy^2 . We deal with the two cases separately.

In the first case, consider

$$f^{(1)}(x, y) \equiv f(x+1, y) - f(x, y). \quad (11)$$

Compared to f , the degree of $f^{(1)}$ in x is decreased by 1, while its degree in y is the same or smaller. Moreover, it is easy to see

$$\Delta(f^{(1)}) = \Delta(f) - 1 = k \geq 2. \quad (12)$$

Thus by induction $P^{f^{(1)}} \rightarrow PR_p$. Furthermore, $P^{f^{(1)}}$ can be simulated with two copies of P^f as follows: for the first P^f , Alice inputs $x+1$ and Bob inputs y , and assume they receive outputs a_1 and b_1 ; for the second P^f , Alice inputs x and Bob inputs y , and assume they receive outputs a_2 and b_2 . Then Alice sets $a = a_1 - a_2$ as her final output, and Bob sets $b = b_1 - b_2$ as his final output. Then we have

$$\begin{aligned} a - b &= (a_1 - a_2) - (b_1 - b_2) \\ &= (a_1 - b_1) - (a_2 - b_2) \\ &= f(x+1, y) - f(x, y) \\ &= f^{(1)}(x, y). \end{aligned} \quad (13)$$

So $P^f \rightarrow P^{f^{(1)}} \rightarrow PR_p$.

A similar argument holds for the second case. But in this case, we consider

$$f^{(2)}(x, y) \equiv f(x, y+1) - f(x, y), \quad (14)$$

which satisfies

$$\Delta(f^{(2)}) = \Delta(f) - 1 = k \geq 2. \quad (15)$$

Then by induction $P^{f^{(2)}} \rightarrow PR_p$. Furthermore, $P^{f^{(2)}}$ can also be simulated with two copies of P^f . Therefore we have $P^f \rightarrow P^{f^{(2)}} \rightarrow PR_p$.

Remark 9. This proof actually yields a recursive strategy to simulate PR_p with $2^{\Delta(f)-2}$ copies of P^f . To be specific, we have shown

$$P^f \rightarrow P^{f_1} \rightarrow P^{f_2} \rightarrow \dots \rightarrow P^{f_L} \rightarrow PR_p, \quad (16)$$

where $f_i(x, y) = f_{i-1}(x+1, y) - f_{i-1}(x, y)$ or $f_i(x, y) = f_{i-1}(x, y+1) - f_{i-1}(x, y)$. The strategy is to use a P^{f_L} to simulate a PR_p , where this P^{f_L} is simulated with two copies of $P^{f_{L-1}}$, where each copy of $P^{f_{L-1}}$ is simulated with two copies of $P^{f_{L-2}}$, and so on. Overall, $2^{\Delta(f)-2}$ copies of P^f is used, since $\Delta(f_{i-1}) - \Delta(f_i) = 1$ and $\Delta(f_L) = 2$.

This strategy can be demonstrated by the following example. Suppose $p = 3$ and $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ is given by

$$f(x, y) = x^2y^2 + 2xy^2 + xy + 2x. \quad (17)$$

Using two copies of P^f , we can simulate a P^{f_1} where

$$\begin{aligned} f_1(x, y) &= f(x+1, y) - f(x, y) \\ &= 2xy^2 + y + 2. \end{aligned} \quad (18)$$

Then using two copies of P^{f_1} (each of which is simulated with two copies of P^f), we can simulate a P^{f_2} where

$$\begin{aligned} f_2(x, y) &= f_1(x, y+1) - f_1(x, y) \\ &= xy + 2x + 1 \end{aligned} \quad (19)$$

Finally, we can simulate a PR_p with a P^{f_2} by Alice subtracting her output by $2x + 1$. Overall, four copies of P^f is used to to simulate a PR_p .

■

Hence there are only two inequivalent classes of functional boxes with respect to asymptotic transformation: those corresponding to additively separable functions are local and cannot benefit distributed computation, while the others are all equivalent to PR_p and can enable perfect distributed computation and make communication complexity trivial. Therefore, we have

Theorem 10. *In any world where communication complexity is not trivial, the functional box P^f corresponding to any additively inseparable function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ cannot be implemented perfectly.*

III. LIMITS ON NONLOCALITY FROM INFORMATION CAUSALITY

In the previous section, we have shown that an exact implementation of P^f for any additively inseparable function f is impossible, unless communication complexity collapses. So now the question is how well these boxes might be implemented in nature. In this section, we partially answer this question by deriving several bounds on the proximity between any plausible p -nary-input, p -nary-output box and these functional boxes, from the principle of information causality. But before doing that, we need to first present the following result which is a key ingredient to our analysis.

A. Generalized Depolarization Process

It is well known that any binary-input, binary-output box can be transformed into an *isotropic* one:

$$\begin{aligned} P_{iso}(\lambda) &\equiv \lambda PR_2 + (1 - \lambda)P_N \\ &= \frac{1 + \lambda}{2}PR_2 + \frac{1 - \lambda}{2}\overline{PR_2}, \end{aligned} \quad (20)$$

where P_N is the completely random noise (i.e. $P_N(a, b|x, y) = \frac{1}{4}, \forall a, b, x, y \in \mathbb{Z}_2$), and $\overline{PR_2}$ is the anti-PR box (i.e. $\overline{PR_2}(a, b|x, y) = \frac{1}{2}$ if $a + b = xy + 1$, and 0 otherwise, $\forall a, b, x, y \in \mathbb{Z}_2$), via the so-called *depolarization* process[11, 32]: Alice and Bob generate three independent and uniformly random bits α, β and γ , and modify their inputs and outputs by

$$\begin{aligned} x &\rightarrow x + \alpha, \\ y &\rightarrow y + \beta, \\ a &\rightarrow a + \beta x + \alpha\beta + \gamma, \\ b &\rightarrow b + \alpha y + \gamma. \end{aligned} \quad (21)$$

Here we prove an analogue of this result for p -nary-input, p -nary-output boxes.

Definition 11.

$$PR_{p,j}(a, b|x, y) = \begin{cases} \frac{1}{p}, & \text{if } a - b = xy - j \\ 0, & \text{otherwise} \end{cases}, \quad (22)$$

where $a, b, x, y, j \in \mathbb{Z}_p$.

Lemma 12. *Given any p -nary-input, p -nary-output box P , define*

$$\mu_j = \frac{1}{p^2} \sum_{x, y=0}^{p-1} P(a - b = xy - j|x, y), \quad (23)$$

where

$$P(a - b = xy - j|x, y) = \sum_{k=0}^{p-1} P(a = k, b = k - xy + j|x, y). \quad (24)$$

Then

$$P \rightarrow \sum_{j=0}^{p-1} \mu_j PR_{p,j}. \quad (25)$$

Proof: Consider the following protocol: Alice and Bob generate three independent and uniformly random variable $\alpha, \beta, \gamma \in \mathbb{Z}_p$. They input

$$\begin{aligned} x' &= x + \alpha, \\ y' &= y + \beta \end{aligned} \quad (26)$$

to box P . Suppose they obtain outputs a' and b' . Then they set

$$\begin{aligned} a &= a' - \beta x - \alpha\beta + \gamma, \\ b &= b' + \alpha y + \gamma \end{aligned} \quad (27)$$

as their final outputs.

Suppose this protocol realizes a box \tilde{P} . Then for any given a, b, x, y ,

$$\tilde{P}(a, b|x, y) = \frac{1}{p^3} \sum_{\alpha, \beta, \gamma=0}^{p-1} P(a', b'|x', y'). \quad (28)$$

Note that

$$\begin{aligned} a' - b' - x'y' &= (a + \beta x + \alpha\beta - \gamma) - (b - \alpha y - \gamma) \\ &\quad - (x + \alpha)(y + \beta) \\ &= a - b - xy. \end{aligned} \quad (29)$$

Besides, (x', y') are uniformly random in $\mathbb{Z}_p \times \mathbb{Z}_p$; a' (or b') is also uniformly random in \mathbb{Z}_p conditioned on any (x', y') . So, if $a - b = xy - j$, then

$$\begin{aligned} \tilde{P}(a, b|x, y) &= \frac{1}{p^3} \sum_{x', y'=0}^{p-1} P(a' - b' = x'y' - j|x', y') \\ &= \frac{\mu_j}{p}, \end{aligned} \quad (30)$$

which implies

$$\tilde{P} = \sum_{j=0}^{p-1} \mu_j PR_{p,j}. \quad (31)$$

■

Hence, any p -nary-input, p -nary-output box can be transformed into a probabilistic mixture of $PR_{p,j}$'s, each of which is essentially equivalent to PR_p up to an additive shift of the outputs.

Remark 13. Lemma 12 can be straightforwardly generalized to the case of any q -nary input/output box where q does not have to be prime.

B. Limits on Nonlocality from Information Causality

Let us briefly review the principle of information causality[18]. It was introduced via the following communication task, which is similar to a random access code [33] or oblivious transfer [6, 34]. Suppose Alice and Bob are two spatially separated parties. Alice receives a string of N random and independent p -nary digits $\vec{x} = (x_0, x_1, \dots, x_{N-1}) \in \mathbb{Z}_p^N$. Bob receives a random variable $y \in \{0, 1, \dots, N-1\}$ and is asked to give the y -th digit of Alice. To achieve this, they may share in advance some no-signalling resources such as shared randomness, entangled states or nonlocal boxes. Besides, Alice is allowed to send at most m p -nary digits (or equivalently, $m \log_2 p$ bits) to Bob. Let us denote Bob's output by b . The degree of their success is quantified by

$$I \equiv \sum_{i=0}^{N-1} I(x_i : b|y = i) \quad (32)$$

where $I(x_i : b|y = i)$ is the Shannon mutual information between x_i and b , under the condition that Bob receives $y = i$. Note that if $P(b = x_i|y = i) = p_i$, then by Fano's inequality,

$$I \geq N \log_2 p - \sum_{i=0}^{N-1} h(p_i) - \sum_{i=0}^{N-1} (1 - p_i) \log_2 (p - 1) \quad (33)$$

where $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary entropy function.

The principle of information causality states that for any physically allowed theories, we must have

$$I \leq m \log_2 p. \quad (34)$$

Both classical and quantum correlations satisfy this condition. However, it is unknown whether all postquantum correlations violate this condition.

Now suppose Alice and Bob share unlimited number of copies of a p -nary-input, p -nary-output box P , and Alice is allowed to send only one p -nary digit to Bob, i.e. $m = 1$. We are going to investigate how P can help them in this task, and presents several limits on P from condition (34).

We will consider the cases of $N \leq p$ and $N \geq p$ separately.

Case 1: $N \leq p$

In this case, Alice receives $\vec{x} = (x_1, x_2, \dots, x_N) \subseteq \mathbb{Z}_p^N$ and Bob receives $y \in \{0, 1, \dots, N-1\} \subseteq \mathbb{Z}_p$. Bob aims to obtain the value of

$$F(\vec{x}, y) \equiv x_y. \quad (35)$$

Note that

$$F(\vec{x}, y) = \sum_{i=0}^{N-1} \left[\prod_{0 \leq j \neq i \leq N-1} (i - j)^{-1} (y - j) \right] x_i \quad (36)$$

for any $\vec{x} \in \mathbb{Z}_p^N$ and $y \in \{0, 1, \dots, N-1\} \subseteq \mathbb{Z}_p$. Moreover, the right-hand side of the above equation has degree $N-1$ in y . So $F(\vec{x}, y)$ can be rewritten as

$$F(\vec{x}, y) = \sum_{k=0}^{N-1} y^k F_k(\vec{x}) \quad (37)$$

for some $F_k : \mathbb{Z}_p^N \rightarrow \mathbb{Z}_p$. This fact suggests a protocol that generates each term $y^k F_k(\vec{x})$ independently and then sums them together. For PR_p , this can be achieved by Alice inputting $F_k(\vec{x})$ and Bob inputting y^k , then the difference between their outputs would be $y^k F_k(\vec{x})$. For a general box P , by lemma 12, it can be converted into a mixture of $PR_{p,j}$ boxes which can be viewed as an imperfect PR_p box with random additive noise. As long as the random noise is not very bad, we can still pretend it to be a PR_p and achieve a high efficiency. So consider the following protocol:

Protocol 1 basicRAC(p, N, c, P, \vec{x}, y)

Setup: p is prime. $N \leq p$. Alice has $\vec{x} \in \mathbb{Z}_p^N$ and Bob has $y \in \{0, 1, \dots, N-1\}$. They share at least $N-1$ copies of a p -nary-input, p -nary-output box P . They also choose $c \in \mathbb{Z}_p$.

- Steps:** 1. Alice and Bob convert each copy of P into a copy of $\tilde{P} = \sum_{j=0}^{p-1} \mu_j PR_{p,j}$ (where μ_j is given by Eq.(23)), using the protocol given in the proof of lemma 12.
2. Alice and Bob use $N-1$ copies of box \tilde{P} as follows: for the k -th box, Alice inputs $F_k(\vec{x})$ (which is given by Eqs.(36) and (37)) and Bob inputs y^k , and suppose they get outputs a_k and b_k respectively, $\forall k = 1, 2, \dots, N-1$.
3. Alice sends $q = \sum_{k=1}^{N-1} a_k + F_0(\vec{x})$ to Bob.
4. After receiving q , Bob outputs $b = q - \sum_{k=1}^{N-1} b_k - c$.
-

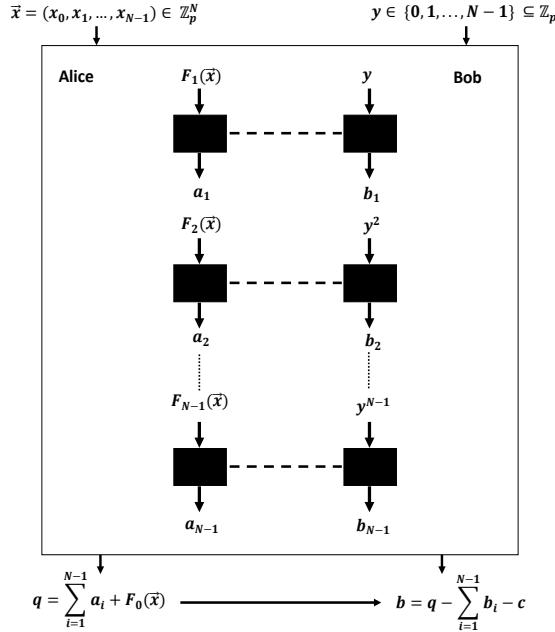


FIG. 1: Basic Protocol for $N \leq p$. Each black box represents a copy of \tilde{P} that is obtained from a copy of P using the protocol given in the proof of lemma 12. $F_0(\vec{x}), F_1(\vec{x}), \dots, F_{N-1}(\vec{x})$ are given by Eqs.(36) and (37).

For an illustration of this protocol, see Fig. 1.

Remark 14. When $p = 2$ and $N = 2$, we have $F(x_0, x_1, y) = x_0 + (x_0 + x_1)y$ and hence $F_1(x_0, x_1) = x_0 + x_1$, $F_0(x_0, x_1) = x_0$. Then the above protocol with $c = 0$ reduces to the basic protocol in Ref.[18].

Let us analyse the efficiency of this protocol.

First, consider the special case of $P = PR_p$ and $c = 0$. In this case, step 1 does not have any effect on PR_p , and

we have $\tilde{P} = PR_p$. So in step 2, we have

$$a_k - b_k = F_k(\vec{x})y^k, \quad \forall k. \quad (38)$$

As a result, Bob's output

$$b = q - \sum_{k=1}^{N-1} b_k = \sum_{k=1}^{N-1} (a_k - b_k) + F_0(\vec{x}) = F(\vec{x}, y). \quad (39)$$

So Bob correctly guesses x_y with certainty.

However, by lemma 12, \tilde{P} is generally not PR_p , but equals $PR_{p,j}$ with probability μ_j , $\forall j \in \mathbb{Z}_p$. Then

$$a_k - b_k = F_k(\vec{x})y^k - j_k \quad (40)$$

where

$$P(j_k = j) = \mu_j, \quad \forall j \in \mathbb{Z}_p. \quad (41)$$

And Bob's output is

$$b = F(\vec{x}, y) - \sum_{k=1}^{N-1} j_k - c, \quad (42)$$

which is correct if and only if

$$\sum_{k=1}^{N-1} j_k = -c, \quad (43)$$

which happens with probability

$$\chi_p(\vec{\mu}, N-1, c) \equiv \sum_{j_1 + \dots + j_{N-1} = -c} \prod_{k=1}^{N-1} \mu_{j_k}, \quad (44)$$

where $\vec{\mu} = (\mu_0, \mu_1, \dots, \mu_{p-1})$. Note that this probability is independent of y . So by Eq.(33), we must have

$$\chi_p(\vec{\mu}, N-1, c) \leq \Theta_p^{-1}\left(\frac{N-1}{N} \log_2 p\right), \quad (45)$$

where

$$\Theta_p(x) = h(x) + (1-x) \log_2(p-1) \quad (46)$$

and $\Theta_p^{-1}(\cdot)$ is its inverse function [35], for condition (34) to be satisfied.

Note that $\forall c \in \mathbb{Z}_p, \forall M \geq 1$,

$$\begin{aligned} \chi_p(\vec{\mu}, M, c) &= \sum_{j_1 + \dots + j_M = -c} \prod_{k=1}^M \mu_{j_k} \\ &= \frac{1}{p} \text{tr}(Z_p^c (\sum_{j=0}^{p-1} \mu_j Z_p^j)^M) \\ &= \frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} (\sum_{j=0}^{p-1} \mu_j \omega_p^{jk})^M. \end{aligned} \quad (47)$$

where $Z_p = \text{diag}(1, \omega_p, \dots, \omega_p^{p-1})$ is the p -dimensional generalization of Pauli Z matrix, $\omega_p = e^{i2\pi/p}$, and in the second step we use $\text{tr}(Z_p^i) = 0, \forall i = 1, 2, \dots, p-1$. Therefore,

Theorem 15. In any world where information causality holds, any p -nary-input, p -nary-output box P satisfies: $\forall N \leq p, \forall c \in \mathbb{Z}_p$,

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} (\sum_{j=0}^{p-1} \mu_j \omega_p^{jk})^{N-1} \leq \Theta_p^{-1}\left(\frac{N-1}{N} \log_2 p\right), \quad (48)$$

where μ_j is defined as Eq.(23).

Case 2: $N \geq p$

Assume $N = p^n$ and $y = \sum_{i=0}^{n-1} y_i p^i$ for $y_i \in \mathbb{Z}_p$. We present a recursive protocol that calls the basicRAC protocol as a subroutine. It is the p -dimensional generalization of the one given in Ref.[18].

Protocol 2 recursiveRAC(p, N, c, P, \vec{x}, y)

Setup: p is prime. $N = p^n$ for some $n \geq 1$. Alice has

$\vec{x} \in \mathbb{Z}_p^N$ and Bob has $y = \sum_{i=0}^{n-1} y_i p^i$ where $y_i \in \mathbb{Z}_p$.

They share at least $N - 1$ copies of a p -nary-input, p -nary-output box P . They also choose $c \in \mathbb{Z}_p$.

Steps: If $N = p$, then Alice and Bob execute basicRAC(p, N, c, P, \vec{x}, y). Otherwise:

- **Alice:** she divides her input \vec{x} into $\frac{N}{p}$ substrings: $\vec{z}_0 \equiv (x_0, x_1, \dots, x_{p-1})$, $\vec{z}_1 \equiv (x_p, x_{p+1}, \dots, x_{2p-1})$, ..., $\vec{z}_{\frac{N}{p}-1} \equiv (x_{N-p}, x_{N-p+1}, \dots, x_{N-1})$. For $k = 0, 1, \dots, \frac{N}{p} - 1$, she executes her part of basicRAC($p, p, c, P, \vec{z}_k, y_0$), except that she does not send her message (which is denoted by q_k). Then she executes her part of recursiveRAC($p, \frac{N}{p}, 0, P, \vec{q}, y'$), where $\vec{q} = (q_0, q_1, \dots, q_{\frac{N}{p}-1})$ and $y' = \sum_{i=1}^{n-1} y_i p^{i-1}$.
 - **Bob:** he executes his part of recursiveRAC($p, \frac{N}{p}, 0, P, \vec{q}, y'$). (Here still $y' = \sum_{i=1}^{n-1} y_i p^{i-1}$.) Suppose the output from this protocol is \hat{q} . Then he executes his part of basicRAC($p, p, c, \vec{z}_{y'}, y_0$), except that he uses \hat{q} as the message received from Alice. The output from this protocol is set as his final output.
-

Fig. 2 illustrates an example of this protocol for $p = 3$ and $N = 9$.

The recursiveRAC protocol can be viewed as a level- n pyramid of basicRAC protocols. Its idea is that Alice uses level $k + 1$ to transmit her messages generated at level k , while Bob uses level $k + 1$ to reveal the message he needs at level k , $\forall k = 0, 1, \dots, n - 1$. Although Alice accesses totally $(p - 1) \sum_{k=0}^{n-1} p^k = N - 1$ copies of \tilde{P} , Bob only accesses $n(p - 1)$ copies of \tilde{P} and only these boxes are truly relevant to his final output. Each of these boxes contributes to his final output an additive shift that equals j with probability μ_j , $\forall j \in \mathbb{Z}_p$. So Bob's final guess is correct if and only if all these additive shifts

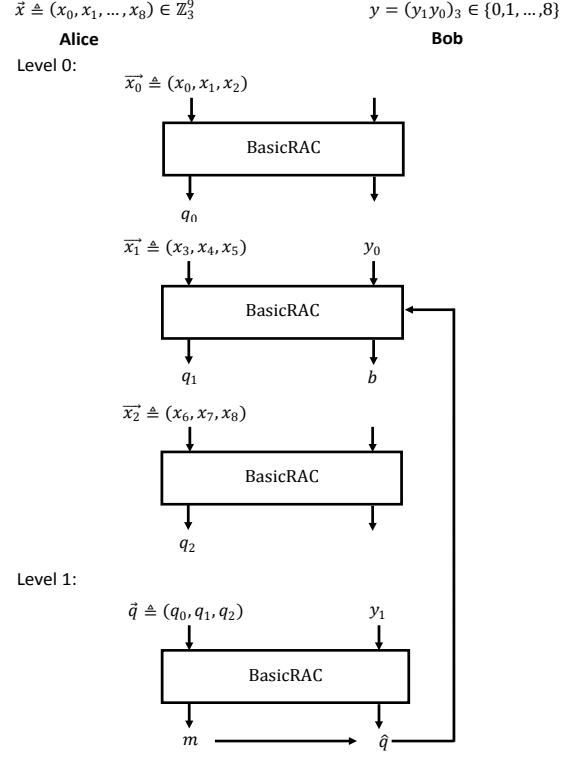


FIG. 2: Recursive protocol for $N \geq p$. Here we show an example for $p = 3$ and $N = 9$. Suppose Alice receives $\vec{x} = (x_0, x_1, \dots, x_8) \in \mathbb{Z}_3^9$ and Bob receives $y = (y_1 y_0)_3 \in \{0, 1, \dots, 8\}$. They also share at least $N - 1 = 8$ copies of some box P . The protocol consists of three level-0 and one level-1 executions of the basic protocol illustrated in Fig.1. For Alice, she executes the three level-0 basic protocols with inputs (x_0, x_1, x_2) , (x_3, x_4, x_5) and (x_6, x_7, x_8) respectively. Suppose her messages (which are not really sent) are q_0, q_1, q_2 respectively. Then she executes the level-1 basic protocol with input (q_0, q_1, q_2) , and truly sends her message for this one. For Bob, he executes the level-1 basic protocol with input y_1 , and suppose his output is \hat{q} . Then he executes only the y_1 -th level-0 basic protocol with input y_0 (this figure shows the case $y_1 = 1$). During this protocol he pretends that \hat{q} is the message received from Alice. At last, this basic protocol's output b is set as Bob's final output. Note that each basic protocol costs $p - 1 = 2$ copies of box P , so Alice totally accesses 8 copies of P , while Bob only accesses 4 copies of P .

sum to $-c$, which happens with probability

$$\begin{aligned} \chi_p(\vec{\mu}, n(p-1), c) &= \sum_{j_1 + \dots + j_{n(p-1)} = -c} \prod_{k=1}^{n(p-1)} \mu_{j_k} \\ &= \frac{1}{p} \sum_{k=0}^{p-1} \omega^{ck} \left(\sum_{j=0}^{p-1} \mu_j \omega^{jk} \right)^{n(p-1)}. \end{aligned} \quad (49)$$

So, by Eq.(33), we must have

$$\chi_p(\vec{\mu}, n(p-1), c) \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right), \quad (50)$$

otherwise condition (34) is violated. Thus,

Theorem 16. *In any world where information causality holds, any p -nary-input, p -nary-output box P satisfies: $\forall n \geq 1, N = p^n, \forall c \in \mathbb{Z}_p$,*

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} \left(\sum_{j=0}^{p-1} \mu_j \omega_p^{jk} \right)^{n(p-1)} \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right), \quad (51)$$

where μ_j is defined as Eq.(23).

1. Bounds with respect to general functional boxes

Theorems 15 and 16 can be viewed as giving bounds on the proximity between a plausible p -nary-input, p -nary-output box and PR_p . By lemma 8, P^f and PR_p are interconvertible for any additively inseparable function f . So there should be also bounds on the proximity between a plausible p -nary-input, p -nary-output box and the corresponding functional box. In what follows, we will give several such bounds.

Definition 17. For any function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, define

$$P_j^f(a, b|x, y) = \begin{cases} \frac{1}{p}, & \text{if } a - b = f(x, y) - j \\ 0, & \text{otherwise} \end{cases}, \quad (52)$$

where $a, b, x, y, j \in \mathbb{Z}_p$.

P_j^f and P^f are essentially equivalent, except for an additive shift of the outputs.

We will consider the case of $\Delta(f) = 2$ and $\Delta(f) > 2$ separately.

Case 1: $\Delta(f) = 2$.

Suppose

$$f(x, y) = \lambda xy + g(x) + h(y) \quad (53)$$

for some $\lambda \neq 0$ and $g, h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$.

Given any p -nary-input, p -nary-output box P , define

$$\nu_j = \frac{1}{p^2} \sum_{x, y=0}^{p-1} P(a - b = f(x, y) - j|x, y) \quad (54)$$

where

$$\begin{aligned} & P(a - b = f(x, y) - j|x, y) \\ &= \sum_{k=0}^{p-1} P(a = k, b = k - f(x, y) + j|x, y). \end{aligned} \quad (55)$$

Then we have

$$P \rightarrow \sum_{j=0}^{p-1} \nu_j P_j^f. \quad (56)$$

To prove this, consider the following protocol: Alice and Bob generate three independent and uniformly random variable $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Alice inputs

$$x' = x + \alpha \quad (57)$$

to P , and Bob inputs

$$y' = y + \beta \quad (58)$$

to P . Suppose they receive outputs a' and b' respectively. Then Alice sets

$$a = a' - \lambda\beta x - \lambda\alpha\beta - g(x + \alpha) + g(x) + \gamma \quad (59)$$

as her final output, and Bob sets

$$b = b' + \lambda\alpha y + h(y + \beta) - h(y) + \gamma \quad (60)$$

as his final output. Suppose this protocol realizes a box \hat{P} . Then for any given a, b, x, y ,

$$\hat{P}(a, b|x, y) = \frac{1}{p^3} \sum_{\alpha, \beta, \gamma=0}^{p-1} P(a', b'|x', y'). \quad (61)$$

Note that

$$\begin{aligned} a' - b' - f(x', y') &= (a + \lambda\beta x + \lambda\alpha\beta + g(x + \alpha) - g(x) \\ &\quad - \gamma) - (b - \lambda\alpha y - h(y + \beta) + h(y) \\ &\quad - \gamma) - (\lambda(x + \alpha)(y + \beta) + g(x + \alpha) \\ &\quad + h(y + \beta)) \\ &= a - b - f(x, y). \end{aligned} \quad (62)$$

Besides, (x', y') are uniformly random in $\mathbb{Z}_p \times \mathbb{Z}_p$; a' (or b') is also uniformly random in \mathbb{Z}_p conditioned on any (x', y') . So, if $a - b = f(x, y) - j$, then

$$\begin{aligned} \hat{P}(a, b|x, y) &= \frac{1}{p^3} \sum_{x', y'=0}^{p-1} P(a' - b' = f(x', y') - j|x', y') \\ &= \frac{\nu_j}{p}, \end{aligned} \quad (63)$$

which implies

$$\hat{P} = \sum_{j=0}^{p-1} \nu_j P_j^f. \quad (64)$$

Now recall that in the proof of lemma 8 we gave the following protocol that converts a P^f to a PR_p : Alice inputs x and Bob inputs y , and suppose they receive a and b . Their final outputs are $a' = \lambda^{-1}(a - g(x))$ and $b' = \lambda^{-1}(b + h(y))$. Note

$$a' - b' - xy = \lambda^{-1}(a - b - f(x, y)). \quad (65)$$

So this protocol converts a P_j^f to a $PR_{p, \lambda^{-1}j}$. Hence, we have

$$\sum_{j=0}^{p-1} \nu_j P_j^f \rightarrow \sum_{j=0}^{p-1} \nu_j PR_{p, \lambda^{-1}j}. \quad (66)$$

Combining Eq.(56) and (66), we obtain

$$P \rightarrow \sum_{j=0}^{p-1} \nu_j PR_{p, \lambda^{-1}j}. \quad (67)$$

Then by theorems 15 and 16, we get

Theorem 18. *In any world where information causality holds, for any additively inseparable function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ with $\Delta(f) = 2$ and any p -nary-input, p -nary-output box P , we have:*

$$\bullet \forall N \leq p, \forall c \in \mathbb{Z}_p,$$

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} \left(\sum_{j=0}^{p-1} \nu_j \omega_p^{jk} \right)^{N-1} \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right); \quad (68)$$

$$\bullet \forall n \geq 1, N = p^n, \forall c \in \mathbb{Z}_p,$$

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} \left(\sum_{j=0}^{p-1} \nu_j \omega_p^{jk} \right)^{n(p-1)} \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right), \quad (69)$$

where ν_j is defined as Eq.(54).

Case 2: $\Delta(f) > 2$.

Given arbitrary p -nary-input, p -nary-output box P , we change it slightly as follows: Alice and Bob generate a uniformly random $\gamma \in \mathbb{Z}_p$, and modify their outputs by $a \rightarrow a + \gamma$ and $b \rightarrow b + \gamma$. Suppose this modified box is P' . They we have

$$P'(a, b|x, y) = \frac{1}{p} E_{x, y, f(x, y) - a + b} \quad (70)$$

where

$$\begin{aligned} E_{x, y, j} &= P(a - b = f(x, y) - j|x, y) \\ &= \sum_{k=0}^{p-1} P(a = k, b = k - f(x, y) + j|x, y). \end{aligned} \quad (71)$$

Define

$$\nu_j = \min_{x, y \in \mathbb{Z}_p} E_{x, y, j}. \quad (72)$$

Then we have

$$P' = \sum_{j=0}^{p-1} \nu_j P_j^f + \left(1 - \sum_{j=0}^{p-1} \nu_j\right) P'' \quad (73)$$

for some box P'' .

Now recall that in the proof of lemma 8, we have given a recursive protocol that transforms $M \equiv 2^{\Delta(f)-2}$ copies of P^f into a copy of PR_p . Let us see what happens if we apply that protocol to P' . Suppose the resulting box is \tilde{P} . Note that P' acts as P_j^f with probability ν_j (or acts as P'' with probability $1 - \sum_{j=0}^{p-1} \nu_j$). So each time Alice and Bob access a P' , their outputs are basically the same as those of P^f except for an additive shift which is j with probability ν_j (or with probability $1 - \sum_{j=0}^{p-1} \nu_j$ the outputs are nonsense). These additive shifts are multiplied by a factor λ^{-1} for some $\lambda \neq 0$ (see Eq.(66)). And the overall shift in the final output is the sum of a half of these

multiplied shifts minus the sum of the other half, since we use a difference method. So,

$$\tilde{P} = \sum_{j=0}^{p-1} \mu_j PR_{p,j} + \left(1 - \sum_{j=0}^{p-1} \mu_j\right) P''', \quad (74)$$

where

$$\mu_j = \sum_{(j_1, \dots, j_M) \in \mathcal{S}_{M,j}} \prod_{k=1}^M \nu_{j_k} \quad (75)$$

in which

$$\mathcal{S}_{M,j} \equiv \{(j_1, \dots, j_M) \in \mathbb{Z}_p^M : \sum_{k=1}^{\frac{M}{2}} j_k - \sum_{k=\frac{M}{2}+1}^M j_k = \lambda j\} \quad (76)$$

and P''' is some box.

Then, by lemma 12, we have

$$\tilde{P} \rightarrow \hat{P} = \sum_{j=0}^{p-1} \hat{\mu}_j PR_{p,j} \quad (77)$$

for some $\hat{\mu}_j \geq \mu_j$.

Now assume Alice and Bob execute basicRAC($p, N, c, \hat{P}, \vec{x}, y$) for $N \leq p$. Then Bob's guess is correct with probability

$$\begin{aligned} \chi_p(\vec{\mu}, N-1, c) &= \sum_{j_1 + \dots + j_{N-1} = -c} \prod_{k=1}^{N-1} \hat{\mu}_{j_k} \\ &\geq \sum_{j_1 + \dots + j_{N-1} = -c} \prod_{k=1}^{N-1} \mu_{j_k} \\ &= \sum_{(j_1, \dots, j_{M(N-1)}) \in \mathcal{S}_{M(N-1), -c}} \prod_{k=1}^{M(N-1)} \nu_{j_k} \\ &\equiv \sigma_p(\vec{\nu}, M(N-1), c), \end{aligned} \quad (78)$$

where in the second step we use $\hat{\mu}_j \geq \mu_j \geq 0$, and in the third step we use Eqs.(75) and (76), and in the last step $\vec{\nu} = (\nu_0, \nu_1, \dots, \nu_{p-1})$. So we must have

$$\sigma_p(\vec{\nu}, M(N-1), c) \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right), \quad (79)$$

otherwise condition (34) is violated.

Similarly, if Alice and Bob execute recursiveRAC($p, N, c, \hat{P}, \vec{x}, y$) for $N = p^n$, then Bob's guess is correct with probability

$$\chi_p(\vec{\mu}, n(p-1), c) \geq \sigma_p(\vec{\nu}, Mn(p-1), c), \quad (80)$$

So unless

$$\sigma_p(\vec{\nu}, Mn(p-1), c) \leq \Theta_p^{-1} \left(\frac{N-1}{N} \log_2 p \right), \quad (81)$$

condition (34) is violated.

Note that $\forall L \geq 1, \forall c \in \mathbb{Z}_p$,

$$\begin{aligned}\sigma_p(\vec{\nu}, L, c) &= \sum_{(j_1, \dots, j_L) \in \mathcal{S}_{L, -c}} \prod_{k=1}^L \nu_{j_k} \\ &= \frac{1}{p} \text{tr}(Z_p^{\lambda c} (\sum_{j=0}^{p-1} \nu_j Z_p^j)^{\frac{L}{2}} (\sum_{j=0}^{p-1} \nu_j Z_p^{-j})^{\frac{L}{2}}) \\ &= \frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{\lambda ck} (\sum_{j=0}^{p-1} \nu_j \omega_p^{jk})^{\frac{L}{2}} (\sum_{j=0}^{p-1} \nu_j \omega_p^{-jk})^{\frac{L}{2}},\end{aligned}\tag{82}$$

where in the second step we use $\text{tr}(Z_p^i) = 0, \forall i = 1, 2, \dots, p-1$. So we have

Theorem 19. *In any world where information causality holds, for any additively inseparable function $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ with $\Delta(f) > 2$ and any p -nary-input, p -nary-output box P , we have:*

$$\bullet \forall N \leq p, L = (N-1)2^{\Delta(f)-2}, \forall c \in \mathbb{Z}_p,$$

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} (\sum_{j=0}^{p-1} \nu_j \omega_p^{jk})^{\frac{L}{2}} (\sum_{j=0}^{p-1} \nu_j \omega_p^{-jk})^{\frac{L}{2}} \leq \Theta_p^{-1}(\frac{N-1}{N} \log_2 p); \tag{83}$$

$$\bullet \forall n \geq 1, N = p^n, L = n(p-1)2^{\Delta(f)-2}, \forall c \in \mathbb{Z}_p,$$

$$\frac{1}{p} \sum_{k=0}^{p-1} \omega_p^{ck} (\sum_{j=0}^{p-1} \nu_j \omega_p^{jk})^{\frac{L}{2}} (\sum_{j=0}^{p-1} \nu_j \omega_p^{-jk})^{\frac{L}{2}} \leq \Theta_p^{-1}(\frac{N-1}{N} \log_2 p), \tag{84}$$

where ν_j is defined as Eqs.(71) and (72).

Remark 20. Since quantum correlations satisfy the principle of information causality, theorems 15, 16, 18 and 19 all apply to them.

IV. CONCLUSION

In summary, we have proposed the class of functional boxes which incorporate the generalized PR boxes as a special case. Every functional box corresponding to an additively inseparable function is asymptotically equivalent to a generalized PR box, which can enable perfect

distributed computation and make communication complexity trivial. So all such functional boxes are unlikely to exist. Furthermore, we investigated how proximate can a general box be to these functional boxes without violating the principle of information causality.

Our work raises many new questions:

First, we have shown that if PR_p box can be implemented exactly, it would lead to the collapse of *deterministic* communication complexity. But we do not know how much noise it can tolerate while still making *probabilistic* communication complexity trivial. And what about general P^f ?

Second, in the proof of lemma 8, we gave a protocol that transforms $2^{\Delta(f)-2}$ copies of P^f into a PR_p . That protocol is universal, but might be not optimal for some f . If we can simulate a PR_p with fewer copies of P^f , then the bounds in theorem 19 can be improved accordingly. In fact, can we directly use P^f to perform distributed computation, instead of first converting it into PR_p ?

Third, as pointed out in Ref.[17], the set of physically allowed boxes should form a closed set under local wirings. Namely, if a set of boxes P_1, P_2, \dots, P_m are all allowed by a physical theory, then a new box \hat{P} obtained by locally connecting these boxes should also be allowed by this theory. Conversely, if \hat{P} is not allowed, then at least one of P_1, P_2, \dots, P_m should be prohibited. Since we have already obtained a set of implausible postquantum correlations, can we use this approach to rule out more?

Finally, here we have only considered bipartite p -nary-input, p -nary-output boxes. It would be interesting to extend our results to more general boxes with arbitrary number of inputs and outputs, as well as multipartite boxes.

Acknowledgments

This research was supported by NSF Grant CCR-0905626 and ARO Grant W911NF-09-1-0440.

-
- [1] J. S. Bell, *Physics* **1**, 195(1964).
 - [2] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969); **24**, 549(E) (1970).
 - [3] B. S. Tsirelson, *Lett. Math. Phys.* **4**, 93 (1980).
 - [4] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
 - [5] W. van Dam, arxiv: quant-ph/0501159.
 - [6] S. Wolf and J. Wullschleger, arxiv:quant-ph/0502030.
 - [7] J. Barrett and S. Pironio, *Phys. Rev. Lett.* **95**, 140401 (2005).
 - [8] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu and D. Roberts, *Phys. Rev. A* **71**, 022101 (2005).
 - [9] H. Buhrman, M. Christandl, F. Unger, S. Wehner and A. Winter, *Proc. Roy. Soc. Lond. A* **462**, 1919 (2006).
 - [10] G. Brassard, H. Buhrman, N. Linden, A. Méthot, A. Tapp and F. Unger, *Phys. Rev. Lett.* **96**, 250401 (2006).
 - [11] L. Masanes, A. Acín and N. Gisin, *Phys. Rev. A* **73**, 012112 (2006).
 - [12] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino and A. Acín, *Phys. Rev. A* **74**, 042339 (2006).
 - [13] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, *Phys. Rev. Lett.* **99**, 240501 (2007).
 - [14] N. Linden, S. Popescu, A. J. Short and A. Winter, *Phys. Rev. Lett.* **99**, 180502 (2007).
 - [15] J. Barrett, *Phys. Rev. A* **75**, 032304 (2007).

- [16] S. Marcovitch and B. Reznik, Phys. Rev. A **77**, 032120 (2008).
- [17] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T. Vértesi, Phys. Rev. A **80**, 062107 (2009).
- [18] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter and M. Żukowski, Nature **461**, 1101 (2009).
- [19] N. Brunner and P. Skrzypczyk, Phys. Rev. Lett. **102**, 160403 (2009).
- [20] P. Skrzypczyk, N. Brunner and S. Popescu, Phys. Rev. Lett. **102**, 110402 (2009).
- [21] J. Allcock, N. Brunner, M. Pawłowski and V. Scarani, Phys. Rev. A **80**, 040103(R) (2009).
- [22] M. Navascués and H. Wunderlich, Proc. Roy. Soc. Lond. A **466**, 881 (2009).
- [23] L-Y. Hsu, arXiv:0912.2582.
- [24] D. Gross, M. Müller, R. Colbeck and O.C.O. Dahlsten, Phys. Rev. Lett. **104**, 080402 (2010).
- [25] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
- [26] M. L. Almeida, J-D. Bancal, N. Brunner, A. Acín, N. Gisin and S. Pironio, Phys. Rev. Lett. **104**, 230404 (2010).
- [27] D. Cavalcanti, A. Salles and V. Scarani, Nature Communications **1**, 136 (2010).
- [28] Y. Xiang, W. Ren, arXiv:1101.2971.
- [29] L-Y. Hsu, arXiv:1102.5611.
- [30] R. Gallego, L. E. Würflinger, A. Acín and M. Navascués, arXiv:1107.3738.
- [31] S. W. Al-Safi and A. J. Short, arXiv:1107.4031.
- [32] A. J. Short, arXiv:0809.2622.
- [33] A. Ambainis, A. Nayak, A. Ta-Shama and U. Vazirani, J. ACM **49**, 496 (2002).
- [34] M. Rabin, Harvard Aiken Computation Laboratory Technical Report No. TR-81, 1981.
- [35] For any p , the function $\Theta_p(x)$ first monotonically increases, then monotonically drops, as x grows from 0 to 1. Only the first part is interesting to us, and $\Theta_p^{-1}(\cdot)$ is the inverse function for that part.